UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,155	08/24/2001	David Carroll Challener	RPS9 20010045	6294

53493 7590 09/27/2006

LENOVO (US) IP Law
Mail Stop ZHHA/B675/PO Box 12195
3039 Cornwallis Road
RTP, NC 27709-2195

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/940,155	CHALLENER ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on 7/13/06 . Claims 1, 5 and 9 have been amended. Claims 1-12 are pending.

Response to Arguments

2. In response to Applicant's remark in regard to provisionally rejected claims 1-12 under the judicially created doctrine of obviousness double patenting in view of co-pending Application No. 10/748,584 and in view of co-pending Application No. 10/994,620. Applicant states that "Applicant note that if the "Provisional" double patenting rejection is the only rejection remaining in an application (either the present application or in Application No. 10/749,584 or in Application No 10/994,620), then the Examiner should withdraw the rejection and permit that application to issue as a patent. M.P.E.P. 804. The "provisional" double patenting rejection may then be converted into a patent double patenting rejection in the other application at the time the one application issues as a patent. M.P.E.P. 840". However, Since the Provisional Double Patent rejection is *not* the only rejection remaining in the application. Examiner maintains the rejection.

In response to Applicant's response to rejection under 35 U.S.C. 102 (e): Applicant's remark in respect to the cited prior art, Thompson, fails to teach the claimed limitations of claims 1, 5 and 9, "providing protected storage accessible by Basic Input Output System (BIOS) code", "encrypting normally unaccessible (NA) data with said symmetrical encryption key", " (remark, page 3-4). However, Thompson teaches the

encrypted password is compared with stored password after the BIOS program is executed. e.g. "In addition to containing the conventional BIOS program device also contains security program including encryption key and password...the basic concept of the security mechanism is to have a unique password stored in BIOS device and require that password be entered and matched from keyboard or other device at the beginning of each boot (e.g. power-on" (col. 3, lines 48-65). Thus Thompson's teaching of accessing the stored password upon the execution of the BIOS code (e.g. power-on) meets the encrypting and storing NA data accessible by Basic Input Output System (BIOS) code. Stored password being normally un-accessible NA data. Examiner notes that Thompson also teaches password encrypted with public/private key (asymmetric key) or optionally common key (symmetric key) (col. 7, lines 25-28). Thompson teaches that the BIOS device comprises EEPROM, stored password being NA data and BIOS code being ANE data (col. 3, lines 34-35), thus the limitation of "storing said encrypted NA data and accessible non-encrypted (ANE) data in an unprotected electronically erasable programmable read only memory (EEPROM)"(Fig. 3, col. 3, lines 28-67) is met.

In response to Applicant's remark in regard to claim rejection for claims 6-7, Applicant contends that Thompson does not disclose "altering said ANE data by issuing an existing write request to said BIOS from said write protected algorithms for said EEPROM; and updating said ANE data in said EEPROM" (remark, pages 6), As cited in the Office Action, col. 3, lines 27-46. Thompson discloses "...it is electrically alterable and programmable under control of special software, in order to update BIOS over the

life of PC 100. Storage devices of this type are known as programmable read-only memory (PROM), electrically-erasable PROM (EEPROM)...". BIOS is alterable under control of special software in order to update BIOS..." meet the claimed limitation because altering and updating BIOS code through special software encompasses writing program code to modify BIOS code by issuing an existing write request to said BIOS from said write protected algorithm for said EEPROM in order to alter the code and update the BIOS code in the EEPROM.

In response to Applicant's remark in regard to claim rejection for claims 3, 7 and 11. Applicant contends that Thompson fails to teach "accessing said NA data via a change request issued to said BIOS over a secure communication link, validating said change request". Thompson discloses user can request changes of password and verified of user identity over the network communication with trust certification authority (TCA) and changes password stored in BIOS device (col. 6, lines 21-52, "Under the control of the conventional special software for programming BIIOS device, CPU then stores the new encrypted password in password of BIOS"). This encompasses, retrieving the old information, responding to a validated changed request, altering the old password with the new password and storing the new password in BIOS device.

In response to Applicant's response to rejection under 35 U.S.C. 103 (a): Applicant contends that the cited prior art, Thompson and Mirov, taken singly or in combination do not teach or suggest the following claim limitation.

In response to Applicant's remark to rejection on claims 4, 8 and 12. Applicant asserts that Thompson and Mirov, taken singly or in combination do not teach or

suggest "hashing said ANE data and encrypting said hash with said symmetrical encryption key; storing said encrypted hash with said ANE data; computing a hash of configuration data in said ANE data on a boot-up request; decrypting said stored encrypted hash of said configuration data; comparing said decrypted hash of said stored configuration data to said computed hash of said configuration data from said ANE data; booting normally in response to a compare of said decrypted hash and said computed hash; and issuing tamper notification and initiating recovery process on a non-compared of said decrypted hash and said computed hash. Examiner asserts that Thompson discloses that the BIOS code in the PC is stored in an EEPROM that is programmable and be altered and upgrade for the life of the PC and Mirov teaches a the micro-code instruction s contained in the programmable section are re-writable. For example, the programmable section includes a flash memory that is software programmable with new micro-code. The authentication section authenticates the programmable section to verify that the micro-code instructions which boot the computer system are trusted because the programmable section is software programmable" (col. 3, line 55-col. 4, line 7). Mirov teaches hashing the programmable section of the micro-code (ANE data), encrypting the hash with encryption key; Storing the encrypted hash with the programmable micro-code; computing the hash on boot-up; decrypting the encrypted hash; comparing the decrypted hash; booting in response to compared decrypted hash with computed hash; and issue notification to alert in event the hash values does not match (Fig. 3 and 4, col. 4, line 56-col. 5, line 14). Mirov teaches that a flash PROM having an authentication section and a

programmable section affords ease in updating the flash PROM with new micro-code without compromising security, it ensures that the programmable section of the micro-code is proper and authentic. The integrity of the unsecured micro-code is verified when the verification hash matches the data hash and it raised to a level of trusted (col. 5, lines 15-26). Therefore, it would have been an obvious to combine Thompson with Mirov to ensure that programmable and alterable BIOS code stored in EEPROM taught by Thompson receive the authentication stored in the BIOS code device taught by Mirov to raise the level of trust and ensure that when the programmable BIOS code has not been compromised when power-up. For this reason, Examiner asserts that the claimed rejection under U.S.C. 102 and 103 are proper. Therefore, Examiner maintains the rejection.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 5 and 9 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-4 and 8 of copending Application No. 10/749,584 and claims 1, 2, 6 and 7 of copending Application No. 10/994,620 in view of Thompson et al. (U.S. Patent No. 6,725,382).

This is a provisional obviousness-type double patenting rejection.

In respect to claims 1, 5 and 9 of the Instant Application, Applicant recites a method, a computer program product and a computer system claims to provide protected storage accessible by BIOS code; storing a symmetrical encryption key in the protected storage; encrypting normally unaccessible data with the key; storing said encrypted and unencrypted data in EEPROM with write protect algorithms.

Claims 1-4 and 8 of copending Application 10/749,584 claims a modified wake-on-LAN packet using the BIOS over a network (remotely altering data through BIOS); storing the executable code in memory and retrieving the executable code from the memory by an action of BIOS; processing the executable code using the BIOS; verifying the modified wake-on-LAN packet using the BIOS; storing the retrieved executable code to a PARTIES partition of a hard drive associated with the client (storing client associated information in erasable memory). The copending Application fails to recite encrypting the data and storing the encrypted data and the unencrypted data in an EEPROM. However, Thompson teaches a BIOS devices stores BIOS, encrypted password, storing the encryption key and security program in the BIOS device, the

BIOS device can be an electrically erasable EEPROM (Fig. 3 col. 3, line 27-col. 4, line 15). Therefore, it would have been obvious to incorporate the teaching of Thompson's encrypting secure data such as password with encryption key stored in the BIOS accessible storage such as EEPROM (write protected algorithm is inherently required in order to erase data in the EEPROM) instead of hard drive to ensure secure protection to secret data with removable memory storage.

Claims 1 and 2 of the copending Application 10/994,620 recites securely logon to a program using a password; encoding the first password and storing the encoded first password in a Trusted Platform Module; decrypting the encrypted program password; logging to the program with the program password; storing the encrypted program password in a non-volatile memory. In the copending Application, the claim recites storing the encoded password in the Trusted Platform Module (Fig. 1A, Trusted Platform Module interface (encompasses encryption module and decryption module) interfaces with logon module). The copending Application does not recite the protected storage store the encryption key and accessible only by the BIOS and the encrypted password and the unencrypted data stored in EEPROM. However, Thompson discloses encryption is stored in the BIOS device and is accessible by the BIOS and the BIOS device can be an electrically erasable EEPROM (Fig. 3, col. 3, line 27-col. 4, line 15). Therefore, it would have been obvious to incorporate the teaching of Thompson's storing encryption key in the BIOS device with erasable EEPROM instead of hard drive to ensure secure protection to secret data with removable memory storage.

Claims 2-4, 6-8 and 10-12 are also rejected because by their dependency, they contain the language of the independent claims.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5-7 and 9-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Thompson et al. (U.S. Patent No. 6,725,382, hereinafter Thompson).

In respect to claim 1, Thompson discloses a method for securing alterable data in a remotely managed system comprising the steps of:

Providing protected storage accessible only by Basic Input Output System (BIOS) code (see Fig. 3, col. 3, lines 10-26 and lines 47-57);

Storing a symmetrical encryption key in said protected storage (see col. 3, lines 47-57);

Encrypting normally unaccessible (NA) data with said symmetrical encryption key (see Fig. 3, item 306 col. 3, lines 47-57); and

Storing said encrypted NA data and accessible non-encrypted (ANE) data in an unprotected electronically erasable programmable read only memory (EEPROM) with

existing write protected algorithms (see col. 3, line 27-col. 4, line 5, EEPROM, write protected algorithms is inherently required in order for the data stored in the EEPROM to be erased).

In respect to claim 2, Thompson discloses the method of claim 1 further comprising the steps of:

Altering said ANE data by issuing an existing write request to said BIOS from said write protected algorithms for said EEPROMS; and updating said ANE data in said EEPROM (see col. 3, lines 27-46 and col. 7, lines 26-44).

In respect to claim 3, Thompson discloses the method of claim 1, further comprising the steps of:

Accessing said NA data via a change request issued to said BIOS over a secure communication link; Validating said changed request (see Fig. 1, item 130, col. 5, line 45-col. 6, line 67);

Retrieving said symmetrical encryption key by said BIOS in response to said validating change request; Using said symmetrical encryption key to decrypt and alter said NA data; encrypting said altered NA data using said symmetrical encryption key; and storing said altered encrypted NA data in said EEPROM (see col. 3, lines 27-46 and col. 7, lines 25-44).

In respect to claims 5-7 and 9-11, the claimed limitations are computer program product and computer system claims that are substantially similar to method claims 1-3. Therefore, claims 5-7 and 9-11 are rejected based on the similar rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 8 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson (U.S. Patent No. 6,725,382) in view of Mirov et al. (U.S. Patent No. 6,138,236, hereinafter Mirov).

In respect to claim 4, Thompson discloses the method of claim 1. Thompson does not disclose but Mirov discloses the steps of:

Hashing said ANE data and encrypting said hash with said symmetrical encryption key; Storing said encrypted hash with said ANE data; Computing a hash of configuration data in said ANE data on boot-up request; Decrypting said stored encrypted hash of said configuration data; Comparing said decrypted hash of said stored configuration data to said computed hash of said configuration data from said ANE data; Booting normally in response to a compare of said decrypted hash and said computed hash and Issuing tamper notification and initiating recovery processes on a non-compare of said decrypted hash and said computed hash (see Mirov, col. 2, lines

21-32 and col. 3, line 55-col. 5, line 50). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Thompson's password based security program with Mirov's teaching of implementing hashing system to authenticate plurality of micro-code to authorize execution of micro-code to ensure the integrity of the stored data or the programmable micro-code (BIOS code) or affords ease in updating the flash PROM with new micro-code without compromising security (Mirov col. 5, lines 15-19).

In respect to claims 8 and 12, the claimed limitations are computer program product and computer system claims that are substantially similar to method claim 4. Therefore, claims 8 and 12 are rejected based on the similar rationale.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-3962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TT
September 21, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100